DATE(S) ISSUED:

04/12/2011

SUBJECT:

Vulnerability in .NET Framework Could Allow Remote Code Execution (MS11-028)

OVERVIEW:

A vulnerability has been discovered in the Microsoft .NET Framework which could allow an attacker to take complete control of an affected system. Microsoft.NET is a software framework for applications designed to run under Microsoft Windows. This vulnerability may be exploited if a user visits or is redirected to a malicious web page while using a Web browser that supports XAML Browser Applications (XBAPs). XAML Browser Applications are applications designed to run in a web browser, utilizing portions of Web Services as well as rich-client (Windows Forms) technologies.

The vulnerability could also allow an attacker to execute remote code on a Microsoft IIS server if it is configured to run ASP.NET applications.

Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:

• Windows XP

• Windows Vista

• Windows Server 2003

• Windows Server 2008

• Windows 7

• Microsoft .NET Framework 2.0

• Microsoft .NET Framework 3.5

• Microsoft .NET Framework 3.5.1

• Microsoft .NET Framework 4.0

RISK:

Government:

• Large and medium government entities: **High**

• Small government entities: **High**

Businesses:

- Large and medium business entities: **High**

- Small business entities: **High**

Home users: High

DESCRIPTION:

Microsoft .NET is Microsoft's managed code programming model for applications. Microsoft .NET consists of a common language runtime (CLR) and framework code library. A remote code execution vulnerability has been discovered in Microsoft .NET Framework that may allow malicious Microsoft .NET applications to execute arbitrary unmanaged code. This vulnerability can be exploited through three possible attack scenarios. In the first scenario, users can be exploited if they visit a specially crafted web site that hosts malicious XAML (Extensible Application Markup Language) Browser Applications (XBAPs). Please note that the victim must view the malicious site using a web-browser which supports XBAPs. In the second scenario, an attacker uploads malicious ASP.NET code to a web server that hosts user-created content, such as a web-hosting provider. Finally, workstations and servers that are running untrusted Windows .NET applications are also at risk from this vulnerability.

In a web server attack scenario, the attacker would gain the same privileges as the service account associated with the application pool identity. Depending on the privileges granted to the service account and on application pool configuration, an attacker may be able to take control of other application pools on the affected system. In the case of web-browsing attack scenarios, successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the service account, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Microsoft has listed several workarounds that would prevent the vulnerabilities from being exploited on affected systems prior to the patch being applied. These workarounds include disabling partially trusted .NET applications and disabling XAML browser applications in Internet Explorer. Please note that these workarounds could negatively affect business operations.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.

- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.

- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

- Apply the principle of Least Privilege to all services.

- Consider disabling Microsoft .NET applications.

- Consider disabling XAML browser applications in Internet Explorer.

REFERENCES:

Microsoft:

http://www.microsoft.com/technet/security/bulletin/ms11-028.mspx

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3958

Securityfocus:
http://www.securityfocus.com/bid/47223